

E-Government Act of 2002

This document is an introduction to the E-Government Act and explains what parts of the Act specifically address security and how it affects the Department of Education and FSA.

In November 2002, the E- Government Act of 2002 passed. The purposes of the Act include:

- Provide effective leadership of E-Gov efforts by establishing an Administrator of new Office of Electronic Government in OMB.
- Promote Internet usage to increase Government/Citizen interaction.
- Promote interagency collaboration in providing E-Gov services.
- Promote access to high quality government info and services across multiple channels.
- Make Federal Government more transparent and accountable.

The full text is at http://www.cio.gov/documents/e_gov_act_2002.pdf.

The main provisions that relate specifically to security include the following:

Information Security (Title II, FISMA)

- Provides effective Government wide management and oversight of IT security risks including coordination of IT security efforts throughout the civilian, national security, and law enforcement communities.
- Requires agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information collected or maintained or information systems used.
- Requires that each agency report on its information security activities in budget and management reports and requires each agency perform an annual independent evaluation of the information security program by either its Inspector General or an independent auditor.

Federal Information Security Incident Center

- Directs OMB to oversee a central Federal information security incident center which will:
 - Provide timely assistance to agencies;
 - Compile and analyze information security incident information; and
 - Inform agencies about security threats and vulnerabilities.

Inventory of Major Information Systems

- Requires each Agency to develop and maintain an inventory of major information systems.
- Provides that the inventory include an identification of the interfaces between each system, and all other systems or networks, including those not operated by or under the control of the agency.

Confidential Information Protection and Statistical Efficiency

- Requires that OMB coordinate and oversee the confidentiality and information sharing policies and rules established by the various agencies.
- Protects the confidentiality interest of individuals or organizations that provide information for federal statistical programs.
- Allows disclosure only when it will be used by agencies for statistical purposes, when approved by an agency head and where law does not otherwise prohibit it.

Privacy Impact Assessment (Section 208)

FSA responsibilities:

- Perform a privacy impact assessment before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or initiating a new collection of information that— (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual.
- Send the PIA to the CIO.
- If possible the agency is supposed to post the PIA on the website, Federal Registry, etc.

Privacy Protections on Agency Websites (Section 208)

- The Director of the agency will develop guidance on privacy notices to be posted on agency websites.
- Privacy notices should be posted on websites that gather information from the public.

Department of Education Responsibilities for the E-Gov Act:

- Provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information collected or maintained or information systems used.
- Report on its information security activities in budget and management reports
- Perform an annual independent evaluation of the information security program by either its Inspector General or an independent auditor.
- Develop and maintain an inventory of major information systems.

- If possible the agency is supposed to post the PIA on the website, Federal Registry, etc.
- The Director of the agency will develop guidance on privacy notices to be posted on agency websites.

FSA Responsibilities for the E-Gov Act and What FSA has done to Fulfill Them:

- FSA created a privacy impact assessment template for systems to complete.
- FSA created a new line item in the system security process guide that the new systems have to review the privacy impact assessment and complete it if necessary.
- The privacy impact assessment has a section that addresses creating and posting privacy notices on the web.
- FSA will send the privacy impact assessments to the main Department.
- FSA works with the IG to perform yearly security audits.